**From:** Telstra Security Operations **To:** nbn Team (nbn@email)

**Subject:** CRITICAL Spring4Shell RCE Attack - NBN Connection Infrastructure Compromised **Body:**

Hello nbn Team,

At **2022 03 20T03 16 34Z**, our Security Operations Centre detected a critical Spring4Shell

CVE 2022 22965) remote code execution attack targeting your NBN Connection infrastructure (nbn.external.network).

# Incident Summary

* **Threat Type:** Spring4Shell CVE 2022 22965 - Critical RCE vulnerability CVSS 9.8
* **Affected System:** NBN Connection service running Spring Framework 5.3.0
* **Target Host:** nbn.external.network
* **Current Status:** Service functionality **impaired** - immediate attention required
* **Attack Timeline:** 499 exploitation attempts over 5 minutes 03 16 34Z 03 21 00Z

# Technical Details

* **Vulnerability Exploited:** Spring Framework data binding vulnerability on JDK 9
* **Attack Method:** Malicious POST requests to /tomcatwar.jsp endpoint
* **Payload:** Class loader manipulation targeting Tomcat AccessLogValve configuration
* **Result:** Successful deployment of JSP webshell with remote command execution capabilities
* **Firewall Status:** All 499 requests marked as "bypass" - controls circumvented
* **Infrastructure Priority: P1 Critical** service compromised

# Attack Pattern Analysis

* **Peak Activity:** 124 attempts at 03 17 UTC (highest intensity)
* **Gradual Decline:** Attack intensity decreased over the 5-minute window
* **Source Country:** Australia AU - multiple attacker IP addresses
* **Protocol Used:** HTTP/1.1 POST requests with malicious data binding payloads

# Immediate Actions Required

**URGENT** This is a **time-sensitive P1 Critical incident** requiring immediate response:

* **Isolate Infrastructure:** Immediately disconnect nbn.external.network from production
* **Patch Spring Framework:** Upgrade to Spring Framework 5.3.18+ or 5.2.20+ versions
* **Remove Webshells:** Search for and remove tomcatwar.jsp and any other suspicious JSP files
* **Forensic Analysis:** Review system logs for signs of command execution and lateral movement
* **Coordinate Response:** Contact Security Operations immediately for containment guidance

# Supporting Resources

## Official Advisories:

* [CISA Spring4Shell Advisory](https://www.cisa.gov/news-events/alerts/2022/04/01/spring-releases-security-updates-addressing-spring4shell-and-spring-cloud-function-vulnerabilities)
* [Spring Security CVE 2022 22965](https://spring.io/security/cve-2022-22965)
* [Unit 42 Spring4Shell Analysis](https://unit42.paloaltonetworks.com/cve-2022-22965-springshell/)

## Technical References:

* [Microsoft Spring4Shell Guidance](https://www.microsoft.com/en-us/security/blog/2022/04/04/springshell-rce-vulnerability-guidance-for-protecting-against-and-detecting-cve-2022-22965/)
* [Rapid7 Mitigation Guide](https://www.rapid7.com/blog/post/2022/03/30/spring4shell-zero-day-vulnerability-in-spring-framework/)

# Risk Assessment

## CRITICAL IMPACT

* Remote code execution capability established on P1 Critical infrastructure
* High-speed NBN service disruption affecting customer connectivity
* Potential for data exfiltration and further system compromise
* Risk of lateral movement within network environment

The vulnerability allows attackers to execute arbitrary commands on your NBN service infrastructure through class loader manipulation, potentially leading to complete system compromise.

Please initiate your **emergency incident response protocol immediately** and coordinate with Security Operations for technical assistance with containment and remediation activities.

For any questions or issues, don't hesitate to reach out to us. Kind regards,

Telstra Security Operations